RECEIVED
CENTRAL FAX CENTER
JUN 23 2009

Amendments to the Claims

The listing of claims presented below will replace all prior versions, and listings, of claims in the application.

Listing of claims:

1. (**currently amended**) A method for the detection and prevention of intrusions into a computer network with a firewall, the method comprising:

detecting the connections at a central point and before each branch of said network,

selective filtering of the said connections, where said selective filtering stage includes firstly a stage for automatic recognition of the accessing protocol, independently of the communication port used by the said protocol, and secondly, after said accessing protocol has been recognized automatically, a stage for verifying the conformity of each communication flowing in a given connection to the said protocol, to deliver a dynamic authorization for communications resulting from normal operation of the protocol and to deliver a dynamic rejection for communications resulting from abnormal operation of the protocol,

wherein said check on conformity is performed layer by layer, by successive protocol analysis of each part of the data packet flowing in the connection corresponding to a given protocol, from the lowest protocol to the highest protocol, and

wherein, since each main connection enabled is able to induce one or more secondary connections, said check on conformity detects the data necessary for opening said secondary connections and **dynamically** attaches said secondary connections to the authorization for connection of said main connection.

2. (previously presented) A method according to claim 1, wherein, as long as the accessing protocol of a connection is not recognized, the data are accepted but not transmitted.

3. (previously presented) A method according to claim 2, wherein, if the number of data packets accepted but not transmitted exceeds a certain threshold, or if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed.

4. (previously presented) A method according to claim 2, wherein if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed.

5. (previously presented) A method according to claim 2, wherein, when the accessing protocol of a connection is not automatically recognized, said step of checking on conformity of each communication flowing in a given connection to said protocol is replaced by a step of generic checking of coherence of data packets.

6. **(currently amended)** A device for the detection and prevention of intrusions into a computer network, comprising:

a firewall,

a resource for preventing intrusions by detection of the connections, directly incorporated into said firewall at a central point and before each branch of said network, where said resource for the prevention of intrusions includes a resource for selective filtering of said connections by automatic recognition of the accessing protocol, independently of the communication port used by said protocol,

wherein said selective filtering resource includes at least one independent module for the analysis of at least one given communication protocol, and

at least one of the independent modules includes:

i. unit for the automatic recognition of a given communication protocol,

ii. unit for verifying the conformity of the communication flowing in a given connection to the said protocol,

iii. means for delivering a dynamic authorization for communications resulting from normal operation of the protocol, and delivering a dynamic

rejection for communications resulting from abnormal operation of the protocol, and

iv. means of transmission of a part of a data packet to an independent analysis module of a hierarchically higher protocol, **and wherein said unit for verifying the conformity of the communication flowing in a given connection, called main connection, to the said protocol, comprising means of detection of the data necessary for opening secondary connections induced by said main connection, and of attachment of said secondary connections to the authorization for connection of said main connection**.

7. (previously presented) A device according to claim 6, wherein, in addition to the independent module or modules for the analysis of a given communication protocol, the device includes an independent generic module which attaches itself to the connections for which the protocol has been recognized by none of the other said independent modules.

8. (previously presented) A device according to claim 6, wherein the device includes an interface for entry, by a user, of the criteria that determine the filtering policy.

9. (previously presented) A device according to claim 8, wherein, said interface receives the criteria specified in natural language by the user.

10. (previously presented) A device according to claim 9, wherein said criteria specified in natural language include at least one protocol name.

11. (previously presented) A device according to claim 8, wherein said interface allows the activation or deactivation of each of said independent modules.

12. (previously presented) A device according to claim 6, wherein the device includes a resource for statistical processing of the connection data, and a resource for storage of said connection data and processed data.